IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA v. LAFON ELLIS	Criminal No. 19-369

MOTION TO QUASH SUBPOENA

AND NOW comes the United States of America, by its attorneys, Scott W. Brady, United States Attorney for the Western District of Pennsylvania, and Brendan T. Conway, Assistant United States Attorney for said District, and submits this Motion to Quash. Because the subpoena was improvidently issued, impermissibly broad, seeks information already provided by the government, and is beyond the scope of the discovery rules, the Court should quash the subpoena served on Cybergenetics.

By way of background, on August 21, 2018, the Pittsburgh Bureau of Police (PBP) was searching for a vehicle involved in a homicide. They spotted the vehicle, noted some traffic violations, and attempted to stop the vehicle. Ellis was the driver and sole occupant, and he led the police on a high speed chase that resulted in him crashing into a fire hydrant. He fled on foot, and the police were not able to catch him. Police officers, however, recognized Ellis from previous interactions. A search of the vehicle revealed, among other things, a firearm on the driver's side near the brakes and accelerator. Later DNA testing revealed Ellis's DNA on the firearm.

The DNA testing was conducted by a company called Cybergenetics, and it was analyzed through its TrueAllele software. Ellis has prior convictions as an adult for aggravated robbery (two counts), burglary, and illegal gun possession, and the Grand Jury returned an indictment charging him with violating 18 U.S.C. § 922(g)(1). At the arraignment in this matter, the government provided the defendant with extensive discovery related to Cybergenetics and the TrueAllele software. Cybergenetics also has a publicly available website, https://www.cybgen.com/, which provides a great deal of information about the company and its methodology.

On May 6, 2020, counsel for the government was informed by Cybergenetics that it had received a subpoena related to the above-captioned matter that requested a broad array of materials, much of which was already provided by the government, and also sought to assign the costs of the subpoena to the government. The government was not served with the motion for the subpoena or otherwise provided an opportunity to object, and, therefore, the government filed a motion for service of the motion requesting that the Court issue the subpoena ex parte.

As it turns out, it appears that the defendant did not file a motion seeking to file the motion ex parte, a motion requesting the sealing of the subpoena, or any motion requesting authorization to issue the subpoena. Apparently, the defendant simply filed an order, which the Court signed, and issued the subpoena. The defendant did not explain why the subpoena should be filed ex parte or under seal, and the defendant did not address his inability to pay, the necessity of the material, why the subpoena directed that the material be delivered to defense counsel, rather than the Court, why the material should be delivered not a hearing or at the trial, or any other justification for the subpoena.

Pursuant to Federal Rule of Criminal Procedure 17(c)(2), "the court may quash or modify the subpoena if compliance would be unreasonable or inappropriate." The Court should quash this subpoena, issued ex parte and under seal without a motion, because it is both unreasonable and inappropriate. What is at issue here is the justification for the subpoena, its conflict with Rule 16, its requirement to produce material not contemplated by Rule 17, its call to produce the information to defense counsel rather than the Court, the timing of the production, the requirement to surrender possession of the materials, the assignment of costs, and the scope of the material sought.

First, the Rule 17 subpoena issued to Cybergenetics requests information specifically excluded from production under Rule 17. Pursuant to Federal Rule of Criminal Procedure 17(h), "no party may subpoena a statement of a witness or of a prospective witness under this rule. Rule 26.2 governs the production of the statement." Despite that rule, the subpoena appears to ask for witness statements in the form of emails, correspondence, findings, etc. Thus, to the extent that the subpoenas request any of those categories of information, the subpoena should be modified to exclude them.

Second, the subpoena demands information from the government's expert, but the required expert disclosures are governed by Rule 16(a)(1)(G), and Rule 17(c)(1) does not expand those requirements. Indeed, "[c]ourts must be careful that Rule 17(c) is not turned into a broad discovery device, thereby undercutting the strict limitation of discovery in criminal cases found in Federal Rule of Criminal Procedure 16." United States v. Merlino, 2001 WL 283165, at *5 (E.D. Pa. Mar. 19, 2001) (citing United States v. Cuthbertson, 630 F.2d 139, 146 (3d Cir.1980)). See United States v. Fletcher, 461 F.Supp.2d 1101, 1102-103 (D. Az. 2006). The government has, of course, fully complied with its Rule 16 obligations by providing the defendant with the relevant materials and, thus, Rule 17(c) provides no basis for requiring the production of documents from the government's expert that the government is not required to produce under Rule 16. In fact, Rule 16 was amended, in part, because of abuses of Rule 17(c):

> The distortion of Rule 17(c) that resulted from the desire to use it for discovery purposes was lessened with the 1966 amendments of Rule 16. Any document that might previously have been obtained by defendant through use of a subpoena duces tecum may now be obtained by the defendant by discovery. The availability of Rule 16 makes it almost impossible for a defendant to show good cause for use of Rule 17(c) as a discovery device. Thus, the second sentence of Rule 17(c)(1) can be confined to the rather modest purposes the draftsmen intended when they wrote it into the rule.

Wright and Miller, § 275 Production of Documentary Evidence and Objects—Trial Subpoenas, 2 Fed. Prac. & Proc. Crim. § 275 (4th ed.). As the Supreme Court held, "It was not intended by Rule 16 to give a limited right of discovery, and then by Rule 17 to give a right of discovery in the broadest terms. Rule 17 provided for the usual subpoena ad testificandum and duces tecum, which may be issued by the clerk, with the provision that the court may direct the materials designated in the subpoena duces tecum to be produced at a specified time and place for inspection by the defendant. Rule 17(c) was not intended to provide an additional means of discovery. Its chief innovation was to expedite the trial by providing a time and place before trial for the inspection of the subpoenaed materials." Bowman Dairy Co. v. United States, 341 U.S. 214, 220 (1951). Thus, the Court should quash the subpoena because it seeks production beyond the Rule 16 requirements.

Third, the subpoena requests information already provided by the government. The government made an extensive production of material from Cybergenetics to the defense. Yet, the subpoena requests for production of much of that same material. Thus, the Court should require the defendant to modify this subpoena to exclude information already provided by the government. Requiring production of material already provided is unnecessary and unreasonable.

Fourth, based on counsel for the government's review of the subpoena, the defense has demanded production of the material to the defense, as opposed to the Court, which is also not contemplated by Rule 17. Rule 17(c)(1) governs the production of documents. It provides that the "court may direct the witness to produce the designated items **in court** before trial or before they are offered into evidence. When the items arrive, the Court may permit the parties and their attorneys to inspect all or part of them" (emphasis added). The subpoena, however, requires production to defense counsel, which is inconsistent with the plain text of Rule 17. As the defendant is demanding production to the defense and not the Court, the request is not consistent with Rule 17 and is unreasonable or inappropriate. Thus, the Court should quash the subpoena.

Fifth, the subpoena directs Cybergenetics to "provide" the requested documents. That demand is also not consistent with Rule 17. "The person to whom the subpoena is directed must have the papers with him at the designated time and place so that they may be used in evidence, but he is not required to surrender possession of them, unless they have been subpoenaed by a grand jury." § 275 Production of Documentary Evidence and Objects—Trial Subpoenas, Wright and Miller, 2 Fed. Prac. & Proc. Crim. § 275 (4th ed.). Thus, once again, the defendant prepared a subpoena inconsistent with the parameters of Rule 17, and therefore the Court should quash it.

Sixth, the subpoena directs that Cybergenetics provide the records within two weeks of receipt of the subpoena, and the scope of the subpoena is incredibly expansive. The expansiveness of the subpoena is contrary to Rule 17(c). Rule 17(c) subpoenas are not to be used as broad discovery devices, but must be reasonably targeted to ensure the production of material evidence. United States v. Tucker, 249 F.R.D. 58, 66 (S.D.N.Y. 2008). See also U.S. v. Fletcher, 461 F.Supp.2d 1101, 1102-103 (D. Az. 2006) ("Rule 17(c) . . . may only be used to obtain materials which would be admissible as evidence in a criminal proceeding. Subpoenas issued pursuant to

Rule 17(c) are not discovery devices and may not be used to expand the scope of Rule 16.") Given the expansiveness of the request, the timing of the compliance with the subpoena is unreasonable or inappropriate. Moreover, the expansiveness of the subpoena is unreasonable and not narrowly tailored, and therefore the Court should quash it.

Seventh, while the Court may authorize the production to the Court (not the defense) in advance of trial, the defendant has the burden of establishing good cause for the early production. In United States v. Iozia, Judge Weinfeld formulated the terms whose showing is required to have production prior to trial:

> (1) That the documents are evidentiary and relevant; (2) That they are not otherwise procurable by the defendant reasonably in advance of trial by exercise of due diligence; (3) That the defendant cannot properly prepare for trial without such production and inspection in advance of trial and the failure to obtain such inspection may tend unreasonably to delay the trial; (4) That the application is made in good faith and is not intended as a general fishing expedition.

13 F.R.D. 335, 338 (S.D. N.Y. 1952). In United States v. Nixon, the Supreme Court quoted Iozia's formulation and explained the admissibility requirement for a subpoena duces tecum in anticipation of trial as requiring the party seeking production to "clear three hurdles: (1) relevancy, (2) admissibility, (3) specificity." 418 U.S. 683 (1974). See also United States v. Cuthbertson, 651 F.2d 189, 192 (3d Cir. 1981); United States v. Messercola, 701 F. Supp. 482, 485 (D.N.J. 1988). "Thus, a subpoena is limited to evidentiary materials, and courts will not allow general requests for categories of only arguably relevant documents[.]" Wright and Miller, § 275 Production of Documentary Evidence and Objects—Trial Subpoenas, 2 Fed. Prac. & Proc. Crim. § 275 (4th ed.). The defendant did not demonstrate "good cause" because he did not even file a motion in support of his ex parte request, which provides another basis for quashing the subpoena.

Eighth, the subpoena directs that all "costs to be borne by the government." Under Rule 17(b), the "process costs and witness fees will be paid in the same manner as those paid for witnesses the government subpoenas." Trial witness fees are typically paid for by the U.S. Marshals Service after submission by either party of the appropriate form. This production, however, is much more expansive than a witness fee and the potential costs are extensive. Cybergenetics currently charges a base license fee of $40,000 for license by crime labs and other interested parties. To the extent that the subpoena directs "all costs to be borne by the government", the only costs contemplated by Rule 17 are witness fees, and those fees should be paid by the U.S. Marshal's Office through the submission by the defense of the appropriate forms. Any additional costs are to be borne by the Public Defender's Office. The defendant, of course did not even bother to file a motion in support of his request to issue a subpoena, and therefore has not demonstrated his inability to pay for the costs associated with the subpoena. Thus, the Court should quash the subpoena.

Ninth, the defense provided no justification for filing whatever he did file ex parte or under seal. Courts are supposed to be open to the public, and parties are to file pleadings publicly unless there is a justification for filing them under seal. Additionally, pleadings are to be served on the other party absent a strong justification to withhold the pleading. In this case, the defendant did not justify filing his documents under seal or ex parte, and there does not appear to be any justification for filing them ex parte or under seal. Rule 17(c) does not ordinarily permit the use of ex parte applications by the government or the defense for subpoenas seeking pre-trial production of documents unless the sole purpose of seeking the documents is for use at trial. United States v. Fox, 275 F. Supp. 2d 1006, 1012 (D. Neb. 2003). Clearly the purpose of this subpoena is not simply for use at trial. While Rule 17(b) contemplates that a motion for trial witnesses may be filed ex parte, Rule 17(c) contains no such provision. In this case there was no justification for filing the motion under seal because the government had already provided the defendant with extensive information related to Cybergenetics. It should have come to a surprise to no one that Cybergenetics contacted the government, and therefore the most obvious benefit for the defense of filing the entire motion ex parte is precluding the government from submitting an objection to scope and other aspects of the subpoena prior to the Court authorizing the issuance of a subpoena. For that reason, the Court should not only quash the subpoena, but it should also unseal all of the filings related to this subpoena or any other documents filed ex parte and under seal without justification See ECF Nos. 29 through 36.

Lastly, and most importantly, the subpoena asks for production of material that is protected by trade secrets, is overbroad, and is not needed. Of particular concern is the request to produce over 170,000 lines of computer source code that is a trade secret developed over more than a decade ago and costing millions of dollars, and that is not needed to determine the reliability of the program.[1]

A little bit of background is needed to understand the issues presented by the subpoena. Cybergenetics developed a program it calls TrueAllele, which is designed to separate the various contributors to DNA samples processed by crime laboratories and assess the likelihood that a contributor matches a known sample. TrueAllele’s method of analysis differs from

[1] The majority of the factual material from this point forward in this motion was taken from information provided by Mark W. Perlin, PhD, MD, PhD. Dr. Mark Perlin is Chief Scientific and Executive Officer at Cybergenetics in a document shared with the defense.

traditional DNA analysis performed by humans in that TrueAllele does not utilize thresholds, which exclude or discard data that falls below a predetermined level. Instead, it analyzes all of the data, taking into account peak heights and other patterns. Thus, TrueAllele yields more accurate results, that is, it can produce a stronger "match statistic" or, alternatively, exclude an individual who may have otherwise been included. State v. Simmer, 935 N.W.2d 167, 174 (2019).

TrueAllele has been used in over 850 criminal cases, with expert witness testimony given in over 90 trials. TrueAllele results have been reported in 44 of the 50 states, including in Pennsylvania. Both prosecutors and defenders use TrueAllele for determining DNA match statistics. TrueAllele is also used by innocence projects and for post-conviction relief. TrueAllele's reliability has been confirmed in appellate precedent in Nebraska, New York, and Pennsylvania. See State v. Simmer, 935 N.W.2d 167 (Neb. 2019); People v. Wakefield, 47 Misc.3d 850, 9 N.Y.S.3d 540, 2015 N.Y. Slip Op. 25037 (N.Y. Supreme Ct. 2015) ("Cybergenetics TrueAllele Casework software, which uses a fully continuous probabilistic approach and is one of, if not, the most advanced method of interpreting DNA profiles from mixed and low-template DNA, is generally accepted as reliable by the scientific community[.]"); and Pennsylvania v. Foley, 38 A.3d 882 (Pa. Super. Ct. 2012) ("Here, we find no legitimate dispute regarding the reliability of . . . proprietary software called TrueAllele to interpret the data . . . received"). See also Katherine L. Moss, The Admissibility of Trueallele: A Computerized DNA Interpretation System, 72 Wash. & Lee L. Rev. 1033, 1070 (2015).

There is no genuine controversy as to the validity and reliability of the TrueAllele method. The TrueAllele calculation is entirely objective: when it determines the genotypes for the contributors to the mixture evidence, the computer has no knowledge of the comparison genotypes.

Genotype comparison and match statistic determination are only done after genotypes have been computed. Moreover, the computer uses all the data, without user intervention. In this way, TrueAllele computing avoids human examination bias, and provides a fair match statistic. Over thirty-five validation studies have been conducted by Cybergenetics and other groups to establish the reliability of the TrueAllele method and software. Eight of these studies have been published in peer-reviewed scientific journals, for both laboratory-generated and casework DNA samples. Source code was not needed or used in any of these studies.

Defendant argues that TrueAllele is a novel and highly criticized technology. However, the TrueAllele software has been admitted into courts, found reliable, and declared to not be a novel scientific technique. A Pennsylvania appellate court upheld admission of testimony based on the interpretation of TrueAllele data against a challenge that it did not meet the Frye standard. Commonwealth v. Foley, 38 A.3d 882, 890 (Pa. Super. Ct. 2012); Frye v. United States, 293 F. 1013 (D.C. Cir. 1923). The Foley court held the defendant failed to establish the existence of a legitimate dispute over the TrueAllele system and failed to show that the testimony constituted novel scientific evidence. Foley, supra, at p. 890.

The TrueAllele software is not novel. In People v. Wakefield, the defendant challenged the trial court's Frye ruling that TrueAllele was generally accepted by the relevant scientific community and not novel. The Wakefield court found the trial court's ruling proper and cited forensics journals, validation studies, peer reviewed publications, and the New York State Forensic Science Commission's binding recommendation that TrueAllele be used by the State Police to show its reliability, historic use, and effectiveness. People v. Wakefield, 47 Misc.3d 850, 9 N.Y.S.3d 540, 2015 N.Y. Slip Op. 25037 (N.Y. Supreme Ct. 2015). In fact, TrueAllele results have become so unquestionably reliable that some defendants, at least in Pennsylvania, have stopped challenging them on appeal. See Commonwealth v. Long, No. 1432 WDA 2017, 2020 WL 603869, at *3 (Pa. Super. Ct. Feb. 7, 2020).

Every court that analyzed whether Cybergenetics should have to reveal its source code has determined that it does not. In Commonwealth v. Knight, No. 379 WDA 2017, 2017 WL 5951725, at *6 (Pa. Super. Ct. Nov. 29, 2017), Pennsylvania's Superior Court held that "the source code for TrueAllele was not material to Appellant's defense and his request to compel its production was not reasonable[.]" The Court reasoned that, "scientists can validate the reliability of a computerized process even if the 'source code' underlying that process is not available to the public." (quoting Foley, 38 A.3d at 889).

In Commonwealth v. Robinson, the court rejected defendant's discovery request for the source code. Commonwealth v. Robinson, 2016 Pa. D. & C. Dec. LEXIS 21764 (Allegheny Co. Ct of Common Pleas Feb. 4, 2016) (attached hereto as Exhibit A). The court found the source code was not material to the defendant's ability to pursue a defense. See also Commonwealth v. Arganda, CC No. 201317748 (Allegheny Co. Ct. Common Pleas June 8, 2016) (attached hereto as Exhibit B) (denying motion for reconsideration of order granting motion to quash subpoena for TrueAllele's source code). Similarly, the court of People v. Superior Court (Chubbs) held that the source code was not necessary to judge the software's reliability and that defendant had not made a prima facie showing of the particularized need for the code. People v. Superior Court (Chubbs) 2015 WL 139069 (Cal. Ct. App. January 9, 2015). See also Washington v. Fair, Case No. 10-1-09274-5 SEA (Super. Ct. of Wa. for King Co. 1/12/1017) (attached hereto as Exhibit C) (denying motion to compel disclosure of TrueAllele's source code); Ohio v. Shaw, Case. No. CR-13-575691

(Oh. Ct. of Common Pleas Cuyahgo Co. Oct. 9, 2014) (attached hereto as Exhibit D) (denying motion to compel production of TrueAllele's source code and concluding that "the TrueAllele methodology and the State's witnesses are reliable without the use of the source code."). The defense failed to cite any authority for the proposition that the Court should order the production of the source code and the government knows of no such authority.

Next, the source code is neither necessary nor material to testing the methodology or reliability of the analysis. TrueAllele has about 170,000 lines of computer source code, written by multiple programmers over two decades. The computer code is dense mathematical text. It can take hours for a person to read through even a few dozen lines of code to decipher what it does. Reading at ten lines per hour would entail eight and a half person-years to review all the source code. It is therefore wholly unrealistic to expect that reading through TrueAllele source code would yield meaningful information.

To understand the complexity of this task, it is helpful to discuss the background of what the defendant is asking for. People write a computer program in a programming language using "source code". This source code is later translated into computer-readable "executable" software. TrueAllele is written in MATLAB (for MATrix LABoratory), a high-level mathematical language for programming and visualizing numerical algorithms made by the MathWorks (Natick, MA). Here is an example of MATLAB source code, simplified from a few lines of the MathWorks built-in "mhsample" function that performs Metropolis-Hastings statistical sampling:

```
U = log(rand(nchain,nsamples+burnin));
for i = 1-burnin:nsamples
   y = proprnd(x0);
```

```
    q1 = logproppdf(x0,y);
    q2 = logproppdf(y,x0);
    rho = (q1+logpdf(y))-(q2+logpdf(x0));
    Ui = U(:,i+burnin);
    acc = Ui<= min(rho,0);
    x0(acc,:) = y(acc,:);
    accept = accept+(acc);
end
```

Thus, source code is written in language that humans are capable of understanding, but only if they are fluent in reading, writing and interpreting the particular language that the program is written in. It would be unrealistic for defense counsel to review and use this code in preparation of their defense.

Further, people can easily copy a computer program if they have its source code and disclosure of this code would bring financial ruin to Cybergenetics. Source code contains the software design, engineering know-how, and algorithmic implementation of the entire computer program. Cybergenetics has invested millions of dollars over two decades to develop its TrueAllele system, the company's flagship product. Although the technology is patented, the source code itself is not disclosed by any patent and cannot be derived from any publicly disclosed source. Patent protection is not automatic, and litigation can cost tens of millions of dollars.

Cybergenetics considers the TrueAllele source code to be a trade secret. Cybergenetics does not disclose the source code to anyone outside the company. In fact, the source code has never been disclosed. The source code is not distributed to employees of Cybergenetics, and copies are not provided to individuals, businesses or government agencies that use or license the software. The fact that the source code is kept secret provides Cybergenetics with a significant advantage over others who do not have access to the source code and do not have the programming know-how or are not willing to make the investment necessary to develop comparable software.

Disclosure of the TrueAllele source code trade secret would cause irreparable harm to the company, enabling competitors to easily copy the company's proprietary products and services. Third party review of source code can divulge proprietary trade secrets wholly unrelated to reliability, but valuable to competitors. Once a review results in a release of hard-earned engineering know-how, that disclosure cannot be reversed. The source code reviewer’s knowledge can be written into other software systems, shared with interested parties, or sold for profit. There are no adequate remedies for redress once this proprietary information has been released. Thus, permitting such individuals to see proprietary information that is immaterial to a case is not reasonable, nor is it in the interest of justice.

Moreover, although the source code for TrueAllele is a secret, the methodology it employs and implements has been disclosed. Cybergenetics has published the core mathematics of TrueAllele’s underlying mathematical model for over 20 years. These publications include scientific papers and patent specifications. Cybergenetics provides a compilation of these mathematical methods in a single summary document. This information discloses TrueAllele’s genotype modeling mechanism, and enables others to understand or replicate the basic method. Indeed, at least five other groups have independently developed software that uses TrueAllele’s linear mixture analysis approach.

In addition, TrueAllele's reliability was established on the evidence in this case. The report and its supporting case packet provided to the defense described the system's sensitivity, specificity and reproducibility on the DNA evidence. The case packet gives the data and parameter inputs used in running the program in the case. The packet also includes a case-specific mini-validation study of reported TrueAllele match statistics, measuring match specificity by comparison with non-contributor genotypes. Source code is not needed to understand or interpret these materials.

Additional discovery material for this case was provided on an optical disc. The DVD contains documents related to TrueAllele's reliability, such as background reading, over thirty validation studies and publications, regulatory approvals, general acceptance, and admissibility rulings. There are tutorial videos that describe TrueAllele methods and explain how the system works, as well as continuing legal education talks. The VUIer™ software for reviewing TrueAllele results is provided (with both Windows and Macintosh installers), along with instructions and user manuals. Case-specific files (data, reports, PowerPoint, case packet, VUIer input) are disclosed, enabling a thorough expert review. Source code is not needed to access these materials, read the files, use the executable VUIer software, or examine the computer results.

WHEREFORE, for the reasons set forth above, the Court should grant the government's motion, quash the subpoena issued to Cybergenetics, and direct the Clerk of Courts to unseal ECF Nos. 29-36.

Respectfully submitted,

SCOTT W. BRADY
United States Attorney

/s/ Brendan T. Conway
BRENDAN T. CONWAY
Assistant U.S. Attorney
PA ID No. 78726